UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/042,505	01/09/2002	Gary J. Cross	AUS920010952US1	6747

35525 7590 04/12/2006

IBM CORP (YA)
C/O YEE & ASSOCIATES PC
P.O. BOX 802333
DALLAS, TX 75380

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 04/12/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/042,505	CROSS, GARY J.	
	Examiner	Art Unit	
	Brandon S. Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 February 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,9-17,19-27,29 and 30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,9-17,19-27,29 and 30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10-27-05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-7, 9-17, 19-27, 29, and 30 are pending in this office action.

2. Applicant's arguments, filed February 22, 2006, have been fully considered but they are not persuasive.

Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 5, 15, and 25 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. Claims 5, 15, and 25 recite the limitation "said application" in limitations 2-4. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

7. Claims 1-7, 9-17, 19-27, 29, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baugh et al. (U.S. Patent No. 5,815,553) in view of Herlin et al. (U.S. Patent No. 5,915,021), and further in view of Ashby et al. (U.S. Patent No. 5,305,384).

Regarding claims 1,11 and 21, Baugh et al. discloses a method/system/computer program product for securing radio transmissions utilizing a conventional radio, said method comprising the steps of:

- Providing a conventional radio, said conventional radio being incapable of encrypting or decrypting signals, said radio including a conventional microphone port that is configured to be coupled to a conventional microphone and a conventional speaker port that is configured to be coupled to a conventional speaker, said radio remaining unmodified (abstract, col. 2, lines 58-62 and fig. 1, ref. num 50, 58, and 62);
- Receiving, within said computer system, an input analog signal from said microphone (col. 2, lines 58-62);
- Encrypting, within said computer system, said input analog signal utilizing public key encryption **to form an encrypted voice file** (col. 8, lines 44-47); and
- Passing said encrypted **voice file** from said computer system to said microphone port that is included within said unmodified radio and transmitting said encrypted **voice file** utilizing said unmodified radio, wherein radio transmissions from said radio are secured (col. 3, lines 9-14 and fig. 1, ref. num 70 and 74).

Baugh et al. does not specifically teach the input signal is encrypted using public key techniques.

Herlin et al. teaches a method for sending a secure message in a telecommunications system using public key encryption (col. 5, lines 12-35 and col. 9, lines 56-58).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine using a public key encryption system, as taught by Herlin et al., with the method/system/computer program product of Baugh et al. It would have been obvious for such modifications because the system gains the advantage of securing the recorded message from unauthorized disclosure by an eavesdropper who is monitoring the communication link. By using public key encryption, the recorded message can only be decrypted by the private key that corresponds to the public key used to encrypt the message (see col. 3, lines 60-67 of Herlin et al.).

The combination of Baugh et al. as modified by Herlin et al. do not specifically teach providing a computer system being separate and apart from said radio.

Ashby et al. teaches providing a computer system coupled between a microphone and said radio, wherein inputs into said radio are received first by said

computer system, said computer system being separate and apart from said radio (fig. 1, ref. num 12, separate from the other components).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine connecting a radio output to a computer input, as taught by Ashby et al., with the method/system/computer program product of Baugh et al./Herlin et al. It would have been obvious for such modifications because encrypting communications from a radio, who is directly connected to a computing device, prevents eavesdropping on police and military communications by encrypting the data directly from the radio (see abstract and col. 1, lines 18-23 of Ashby et al.).

Regarding claims 2,12 and 22, the combination of Baugh et al. as modified by Herlin et al./Ashby et al. teaches further comprising the step of encrypting, within said computer system, said input analog signal utilizing a key pair, said key pair including a public key and a private key (see col. 8, lines 44-47 of Baugh et al. and col. 9, lines 56-58 of Herlin et al.).

Regarding claims 3,13 and 23, the combination of Baugh et al. as modified by Herlin et al./Ashby et al. teaches further comprising the step of encrypting, within said computer system, said input analog signal utilizing said public key (see col. 8, lines 44-47 of Baugh et al. and col. 9, lines 56-58 of Herlin et al.).

Regarding claims 4,14 and 24, the combination of Baugh et al. as modified by Herlin et al./Ashby et al. teaches **wherein the receiving step comprises** receiving, within a first application executing within said computer system, said input analog signal from said microphone; **wherein the encrypting step comprises** encrypting, utilizing said first application, said input analog signal utilizing public key encryption **to form said encrypted voice file**; **wherein the passing step comprises** passing said encrypted **voice file** from said first application to said microphone port of said unmodified radio (see col. 2, lines 58-62, fig. 1, ref. num 50, 58, and 62, col. 3, lines 9-14, fig. 1, ref. num 70 and 74, and col. 8, lines 44-47 of Baugh et al. and col. 9, lines 56-58 of Herlin et al.).

Regarding claims 5, 15 and 25, the combination of Baugh et al. as modified by Herlin et al./Ashby et al. teaches **wherein the receiving step comprises**:

- Converting, by a microphone driver that is executing within said computer system, said input analog signal to a file, said file being in a standard voice file format; constantly monitoring, by said first application, inputs received from said microphone; detecting, by said first application, a receipt of said file (see col. 2, line 63 through col. 3, line 25 of Baugh et al.); and
- **Wherein the encryption step comprises** in response to a detection by said first application of said receipt of said file, encrypting **to form said encrypted voice file**, by said first application utilizing a public key that is part of a public key/private key pair assigned to said computer system (see col. 2, lines 58-62,

fig. 1, ref. num 50, 58, and 62, col. 3, lines 9-14, fig. 1, ref. num 70 and 74, and col. 8, lines 44-47 of Baugh et al. and col. 9, lines 56-58 of Herlin et al.).

Regarding claims 6, 16 and 26, the combination of Baugh et al. as modified by Herlin et al./Ashby et al. teaches further comprising the steps of:

- Providing a second conventional radio, said second conventional radio being incapable of encrypting or decrypting signals, said second radio including a second microphone port that is configured to be coupled to a second conventional microphone and a second speaker port that is configured to be coupled to a second conventional speaker, said second radio remaining unmodified (see fig. 1, ref. num 54, 98, and 102 of Baugh et al.);
- Providing a second computer system coupled between said second speaker and said second unmodified radio, wherein outputs from said second radio are received first by said second computer system before being output to said second speaker, said second computer system being separate and apart from said second radio (see fig. 1, ref. num 12, separate from the other components of Ashby et al.);
- Receiving, within said second computer system, an encrypted output from said second speaker port included within said unmodified second radio (see fig. 1, ref. num 86 of Baugh et al.); and
- Decrypting, within said second computer system, said encrypted output utilizing public key encryption **to form a decrypted output** and outputting said decrypted

output from said second computer system to said second speaker (see col. 8, lines 44-47 of Baugh et al.).

Regarding claims 7,17 and 27, the combination of Baugh et al. as modified by Herlin et al./Ashby et al. teaches **wherein within said second computer system the step of receiving further comprises**:

- Constantly monitoring, by a second application that is executing within said second computer system, said second speaker port (see col. 3, lines 32-42 of Baugh et al.); **and**
- Receiving, by said second application, said encrypted output from said second speaker port (see fig. 1, ref. num 86 of Baugh et al.);
- **Wherein the decrypting step comprises** decrypting, by said second application, said encrypted output utilizing public key encryption (see col. 8, lines 44-47 of Baugh et al.).

Regarding claims 9,19 and 29, the combination of Baugh et al. as modified by Herlin et al./Ashby et al. teaches further comprising the steps of obtaining, by said second computer system, a private key of said computer system; and **wherein the decrypting step further comprises** decrypting said encrypted output utilizing said private key (see col. 2, lines 58-62, fig. 1, ref. num 50, 58, and 62, col. 3, lines 9-14, fig. 1, ref. num 70 and 74, and col. 8, lines 44-47 of Baugh et al. and col. 9, lines 56-58 of Herlin et al.).

Regarding claims 10,20 and 30, the combination of Baugh et al. as modified by Herlin et al./Ashby et al. teaches further comprising the step of exchanging said private key between said computer system and said second computer system prior to **transmitting said encrypted voice file** (see col. 5, lines 31-33 of Herlin et al.).

Response to Arguments

8. Applicant amends claims 1, 4-7, 9-11, 14-17, 19, 21, 24-27, 29, and 30.

9. Applicant argues:

   a. Baugh does not teach a radio including a conventional microphone port that is coupled to a conventional microphone and a conventional speaker port connected to a conventional speaker (page 12 through page 13).

   b. Baugh teaches away from the claimed subject matter (page 13, last paragraph through page 14, first paragraph).

   c. Baugh does not teach converting, by a microphone driver within said computer, said input analog signal to a file, said file being in a standard voice file format (page 15).

   d. Baugh does not teach in response to a detection by said first application of said receipt of said file, encrypting (page 15, last paragraph through page 16).

Regarding argument (a), examiner disagrees with applicant. Ashby shows a conventional radio with the microphone port and speaker port (figure 2 of Ashby).

Baugh shows a computer that receives spoken utterances from an external source (a user) and places them into a first computer (figure 1, reference numbers 58, 62, 50). Connecting the radio and microphone ports of the conventional radio of Ashby to the sound card of Baugh is very well known in the art. Users have been connecting external sources (radios, musical equipment, microphones, any other auxiliary device) to computer sound cards with the intention of capturing the analog signal from the external device, and storing it as a file (perhaps a .wav or .mp3 file for music).

Regarding argument (b), examiner disagrees with applicant. Similar to response (a), Baugh does not teach away from the claimed subject matter. Baugh combined with Ashby teach a combination that is well known in the conventional art that allows auxiliary devices to be connected to a computer and secured.

Regarding argument (c), examiner disagrees with applicant. As discussed in a prior interview with applicant, the spoken data (which is analog) is stored in buffers and then sent to a recipient. However, examiner pointed out previously, and currently, that storing the data in buffers could be replaced by storing the data in files. A conversion inherently takes place by converting the spoken analog voice data into digital data that can be handled and transmitted by a computer. Audio files inputted to a computer and saved are saved as a standard voice file.

Regarding argument (d), examiner disagrees with applicant. Applicant amended claims 5, 15, and 25 to be dependent on claims 1, 11, and 21, respectively. By doing this, there is no antecedent basis for "said application" and therefore the argument is moot. For the sake of furthering the prosecution of the case, examiner still disagrees

with applicant even in light of amending the claims to fix the antecedent basis problems. The receipt of the files takes place when the buffers indicate that they are full. The stored data is encrypted prior to transmission in the case that the voice data is confidential (see col. 5, lines 51-54 of Baugh).

Conclusion

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brenda Bh

BH

CHRISTOPHER REVAK
PRIMARY EXAMINER
CRK 4/9/06